WE CLAIM:

1. A computer security service for a computer network accessible by users and comprising services and resources, the computer security service comprising,

a policy builder component, comprising

a network constituent definition component, for defining user data and services and resources data corresponding to the computer network users, services and resources, and

a policy definition component for defining access policies for the computer network users, services and resources,

a database component for maintaining user, services and resources data, and access policies, and for providing a set of selected access policies in response to a database query, and

a validator component, comprising

a request parser for receiving a policy query for service or resource access originated by a network user and for generating a corresponding database query for submission to the database component, and

a policy parser for receiving the set of access policies provided by the database component in response to the corresponding database query and for generating a policy decision for communication to the network user based on the set of access policies provided by the database component.

2. The security service of claim 1 further comprising an API component for receiving an access request for service or resource access originated by a network user and for passing a corresponding policy query to the validator component, the API component further receiving the policy decision from the validator and accordingly permitting or denying access to the network user.

3. The security service of claim 1 or 2 in which the database component maintains the user, services and resources data, and the access policies in an LDAP compliant format

4. The security service of claim 1 in which the policy definition component comprises a policy definition plug-in integration component for registering one or more policy definition plug-in components for use in defining the access policies.

5. The security service of claim 4 in which the validator component comprises a decision node plug-in integration component for registering one or more decision node plug-in components for use in implementing access policies referencing policy definition plug-in components.

6. The security service of claim 1 in which the validator component comprises an authenticator component for authenticating one or more of the network users.

7. The security service of claim 6 in which the authenticator component comprises an authenticator plug-in integration component for registering plug-ins used in the authentication of the network user.

8. The security service of claim 6 or 7 in which the authenticator component comprises a non-interactive authentication component for the authentication of one or more network users without requiring the one or more network users to interact with the security service.

9. The security service of claim 6 OR 7, ~~or 8~~ further comprising a desktop component for installation on the computer of a network user for use in the authentication of the user.

10. The security service of claim 1 in which the access policies are stored as XML documents and in which the validator component comprises an XML parser.

11. The security service of claim ~~2 or~~ 3 in which the policy query passed by the API component to the validator component is an XML document and in which the validator component comprises an XML parser for parsing the policy query.

12. The security service of claim 10 or 11 in which each XML document is a cryptographically signed XML document.

13. The security service of claim 12 in which the XML documents are encrypted XML documents.

14. The security service of claim 1 in which the policy builder component comprises a graphical user interface for displaying

    a grid having nodes, laid out on a first and on a second axis,

    user labels corresponding to the user data, each user label labelling nodes aligned relative to the first axis of the grid, and

    resource labels corresponding to the services and resources data, each resource label labelling nodes aligned relative to the second axis of the grid,

    the nodes in the grid corresponding to the access policies for users and services and resources, as defined by the user and resource labels.

15. The security service of claim 14, in which the grid comprises a defined set of nodes, aligned relative to the first axis of the grid, each of the defined set of nodes representing the non-interactive authentication characteristic for a unique one of the defined services and resources displayed in the grid.

16. The security service of claim 14, in which the grid comprises a defined set of nodes, aligned relative to the first axis of the grid, each of the defined set of nodes representing the access policy for an unknown user for a unique one of the defined services and resources displayed in the grid.

17. The security service of claim 14, further comprising an access policy editor for defining the nodes in the grid, the access policy editor comprising means for graphically assembling icons representing policy rules to define an access policy for a user-specified node.

18. The security service of claim 1 in which the network constituent definition component further comprises a resource discovery component to poll the

computer network and to generate a resource tree data structure corresponding to resources in the computer network.

19. The security service of claim 18, in which the resource discovery component further comprises a resource discovery plug-in specification component to specify resource discovery plug-in components for carrying out the process of discovery of the resources for a defined service in the network.

20. The security service of claim 1 in which the network constituent definition component further comprises a user discovery component to poll the computer network and to generate a business relationship tree data structure corresponding to users defined for the computer network.

21. The security service of claim 1 in which the security service further comprises means to provide for inheritance of access policies by propagating access policies for network users, services and resources, based on a hierarchical ordering of the user data, and a hierarchical ordering of the services and resources data.

22. The security service of claim 2 or 3 in which the API component is resident on a proxy server.

23. The security service of claim 1 in which the services and resources data is maintained in a resource tree data structure, the resource tree data structure comprising a network entry and label, service and resource entries.

24. The security service of claim 23 in which each entry in the resource tree data structure is permitted to have children entries and in which the data structure is defined such that the network entry is restricted to be the root entry of the data structure, the children of label entries are constrained to be label entries and service entries, the children of service entries are constrained to be resource entries, and the children of resource entries are constrained to be resource entries.

25. A graphical user interface for a security service for a computer network, the computer network comprising defined users, services and resources, the graphical user interface displaying

a grid comprising nodes laid out on a first and on a second axis,

user labels corresponding to defined users, each user label labeling nodes aligned relative to the first axis of the grid,

resource labels corresponding to the defined services and resources, each resource label labeling nodes aligned relative to the second axis of the grid, and

the nodes in the grid corresponding to access policies for the defined users and defined services and resources for the computer network, corresponding to the user and resource labels.

26. The graphical user interface of claim 25 further comprising a user definition component for defining a business relationship tree data structure representing a set of the defined users and in which the user labels displayed by the graphical user interface correspond to the business relationship tree data structure.

27. The graphical user interface of claim 25 further comprising a resource definition component for defining a resource tree data structure representing a set of the defined services and resources and in which the resource labels displayed by the graphical user interface correspond to the resource tree data structure.

28. The graphical user interface of claim 25 further comprising an access policy editor for defining the nodes in the grid, the access policy editor comprising means for graphically assembling icons representing policy rules to define an access policy for a user-specified node.

29. A graphical user interface for a security service for a computer network, the computer network comprising defined users represented by a business relationship tree data structure, the computer network further comprising services and resources, represented by a resource tree data structure, the graphical user interface comprising display means for displaying

a grid comprising nodes laid out on a first axis and on a second axis,

user labels corresponding to the users in the business relationship tree data structure, each user label labelling nodes aligned relative to the first axis of the grid, and

resource labels corresponding to the defined services and resources in the resource tree data structure, each resource label labelling nodes aligned relative to the second axis of the grid,

the nodes in the grid corresponding to access policies for the defined users and defined services and resources, corresponding to the user and resource labels.

30. The graphical user interface of claim 29, the grid comprising inheriting nodes and defining nodes, the defining nodes corresponding to access policies expressly defined by a policy manager, the graphical user interface further comprising means for displaying inherited access policies for inheriting nodes in the grid by propagating access policies from the defining nodes in the grid across the inheriting nodes below the defining nodes in each of the business relationship tree data structure and the resource tree data structure.

31. A policy builder for a security service of a computer network accessible by users and comprising services and resources, the policy builder comprising,

a network constituent definition component, for defining user data and services and resources data corresponding to the computer network users, services and resources, and

a policy definition component for defining access policies for the computer network users, services and resources, the policy definition component comprising,

a plug-in integration component to permit a policy manager to register one or more plug-in components for use in defining manager-defined access policies,

a defined access rule component for providing a set of pre-defined access rules to a policy manager for use in creating access policies.

32. The policy builder of claim 31 further comprising an access policy editor for defining the access policies, the access policy editor comprising means for graphically assembling icons representing the pre-defined access rules and manager-defined access policies.

33. An authentication component for a security service of a computer network, the authentication component comprising,

    a plug-in integration component to permit a policy manager to register one or more plug-in components for use in defining authentication for users of the network and

    a defined authentication component for providing a set of pre-defined authentication methods for use in creating authentication policies.

34. An LDAP server, the LDAP server being operatively connectable with a computer network comprising a set of resources and services, the LDAP server further comprising a network information component for generating, maintaining and providing retrieval from, a tree data structure having nodes corresponding to one or more of the members of the set of resources and services in the computer network.

35. The LDAP server of claim 34, in which the network information component constrains the tree structure to comprise a network entry and label, service and resource entries.

36. The LDAP server of claim 35 in which the network information component permits the entries to have children and constrains the tree structure such that the network entry is restricted to be the root entry of the data structure, the children of label entries are constrained to be label entries and service entries, the children of service entries are constrained to be resource entries, and the children of resource entries are constrained to be resource entries.

37. The LDAP server of claim 34, further comprising a plug-in storage component for

storing plug-in code for defining access policies for the computer network.

38. In a computer network security system, an access policy definition component comprising a rule specification component for defining access policies for hierarchically defined sets of users and for hierarchically defined portions of a computer network, the security policy definition component providing for the propagation of defined security policies for a specified set of users and a specified portion of the computer network, to those sets of users and those portions of the computer network which are located under the specified set of users and under the portion of the computer network, in the respective hierarchies.

39. The security policy definition component of claim 38, further comprising an authentication specification component for the definition of non-interactive authentication for selected members of the set of users.

40. In a computer network security system, an access policy component comprising a policy builder component for generating an XML format representation of an access policy from input from a policy manager, the access policy component storing data corresponding to the XML format representation of the security policy, the access policy component accepting XML format queries relating to defined access policies and generating responses based on the stored data corresponding to defined access policies.

41. In a computer network security system, a validator component and a desktop component,

the desktop component for installation on computers in a computer network utilized by network users, and comprising a desktop authentication component for carrying out authentication of network users in the computer network security system,

the validator component comprising a validator authentication component for the authentication of the network users,

the validator authentication component selectively communicating with the desktop component to carry out authentication of network users, the

authentication being granted on a time-limited basis.

42. In a computer network security system, a validator component comprising a request parser for accepting policy queries in XML format from a user of a computer network, the validator component generating a corresponding database query to a policy database storing a set of access policies for the network, the validator component further comprising a policy parser for accepting XML format access policy definitions and generating a policy definition in XML format to the user.

43. The validator component of claim 42 in which the validator further comprises a plug-in launcher for initiating execution of plug-ins specified in the XML format access policy definitions.

44. A computer program product for use with a computer network, said computer program product comprising a computer usable medium having computer readable program code means embodied in said medium for implementing the computer security service of claim 1, 2, 3, 14, 17, 18, 20, 21, or 23.

45. A computer program product for use with a security service for a computer network, said computer program product comprising a computer usable medium having computer readable program code means embodied in said medium for implementing the graphical user interface of claim 25, 26, or 30.

46. A computer program product for use with a security service for a computer network, said computer program product comprising a computer usable medium having computer readable program code means embodied in said medium for implementing the policy builder of claim 31.

47. A computer program product for use with a security service for a computer network, said computer program product comprising a computer usable medium having computer readable program code means embodied in said medium for implementing the authentication component of claim 33.

48. A computer program product for use with a security service for a computer

network, said computer program product comprising a computer usable medium having computer readable program code means embodied in said medium for implementing the LDAP server of claim 34, 36, 37.

49. A computer program product for use with a security service for a computer network, said computer program product comprising a computer usable medium having computer readable program code means embodied in said medium for implementing an access policy component comprising a policy builder component for generating an XML format representation of an access policy from input from a policy manager, the access policy component storing data corresponding to the XML format representation of the security policy, the access policy component accepting XML format queries relating to defined access policies and generating responses based on the stored data corresponding to defined access policies.

50. A computer program product for use with a security service for a computer network, said computer program product comprising a computer usable medium having computer readable program code means embodied in said medium for implementing a validator component and a desktop component,

the desktop component for installation on computers in a computer network utilized by network users, and comprising a desktop authentication component for carrying out authentication of network users in the computer network security system,

the validator component comprising a validator authentication component for the authentication of the network users,

the validator authentication component selectively communicating with the desktop component to carry out authentication of network users, the authentication being granted on a time-limited basis.

51. A computer program product for use with a security service for a computer network, said computer program product comprising a computer usable medium having computer readable program code means embodied in said medium for implementing a validator component comprising a request parser for accepting

policy queries in XML format from a user of a computer network, the validator component generating a corresponding database query to a policy database storing a set of access policies for the network, the validator component further comprising a policy parser for accepting XML format access policy definitions and generating a policy definition in XML format to the user.

52. A method for providing computer network security, the network being accessible by users and comprising services and resources, the method comprising the steps of:

using a policy builder to define user data and services and resources data corresponding to the computer network users, services and resources, and to define access policies for the computer network users, services and resources,

maintaining user, services and resources data, and access policies, in a database,

providing a set of selected access policies in response to a database query,

receiving, in a validator, a policy query for service or resource access originated by a network user and generating a corresponding database query for submission to the database component, and

receiving, in a validator, the set of access policies provided by the database component in response to the corresponding database query and generating a policy decision for communication to the network user based on the set of access policies provided by the database component.

53. The method of claim 52 further comprising the steps of:

displaying, on a computer display unit, a grid having nodes, laid out on a first and on a second axis,

displaying, on the grid, unit user labels corresponding to the user data, each user label labelling nodes aligned relative to the first axis of the grid, and

displaying on the grid, resource labels corresponding to the services and

resources data, each resource label labelling nodes aligned relative to the second axis of the grid,

whereby the nodes in the grid correspond to the access policies for users and services and resources, as defined by the user and resource labels.

54. A method for displaying access policies for a security service for a computer network, the computer network comprising defined users, services and resources, the method comprising the steps of:

displaying, on a computer display unit, a grid having nodes, laid out on a first and on a second axis,

displaying, on the grid, unit user labels corresponding to the user data, each user label labelling nodes aligned relative to the first axis of the grid, and

displaying on the grid, resource labels corresponding to the services and resources data, each resource label labelling nodes aligned relative to the second axis of the grid,

whereby the nodes in the grid correspond to access policies for the defined users and defined services and resources for the computer network, corresponding to the user and resource labels.

55. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform the method steps of claim 52, 53 or 54.

56. A computer system to provide security for a network accessible by users and comprising services and resources, the computer system comprising,

a policy builder comprising

a network constituent definition component, for defining user data and services and resources data corresponding to the computer network users, services and resources, and

a policy definition component for defining access policies for the computer network users, services and resources, comprising a policy definition plug-in integration component for registering one or more policy definition plug-in components for use in defining the access policies,

a database for maintaining user, services and resources data, and access policies, in an LDAP compliant format, and for providing a set of selected access policies in response to a database query,

a validator, comprising

a request parser for receiving a policy query for service or resource access originated by a network user and for generating a corresponding database query for submission to the database,

a policy parser for receiving the set of access policies provided by the database in response to the corresponding database query and for generating a policy decision for communication to the network user based on the set of access policies provided by the database,

a decision node plug-in integration component for registering one or more decision node plug-in components for use in implementing access policies referencing policy definition plug-in components, and

an API component for receiving an access request for service or resource access originated by a network user and for passing a corresponding policy query to the validator, the API component further receiving the policy decision from the validator and accordingly permitting or denying access to the network user.

57. The computer system of claim 56 in which the validator comprises an authenticator for authenticating one or more of the network users having an authenticator plug-in integration component for registering plug-ins used in the authentication of the network user.

58. The computer system of claim 57 in which the authenticator comprises a non-interactive authentication component for the authentication of one or more network users without requiring the one or more network users to interact with the security service.

59. The computer system of claim 56 in which the policy builder comprises a graphical user interface for displaying

a grid having nodes, laid out on a first and on a second axis,

user labels corresponding to the user data, each user label labelling nodes aligned relative to the first axis of the grid, and

resource labels corresponding to the services and resources data, each resource label labelling nodes aligned relative to the second axis of the grid,

the nodes in the grid corresponding to the access policies for users and services and resources, as defined by the user and resource labels.

60. The computer system of claim 59, in which the grid comprises a defined set of nodes, aligned relative to the first axis of the grid, each of the defined set of nodes representing the non-interactive authentication characteristic for a unique one of the defined services and resources displayed in the grid.

61. The computer system of claim 59, in which the grid comprises a defined set of nodes, aligned relative to the first axis of the grid, each of the defined set of nodes representing the access policy for an unknown user for a unique one of the defined services and resources displayed in the grid.

62. The computer system of claim 59, further comprising an access policy editor for defining the nodes in the grid, the access policy editor comprising means for graphically assembling icons representing policy rules to define an access policy for a user-specified node.

63. The computer system of claim 56 further comprising means to provide for inheritance of access policies by propagating access policies for network users,

services and resources, based on a hierarchical ordering of the user data, and a hierarchical ordering of the services and resources data.